On applications of prehomogeneous vector spaces

【96】

氏名（本籍）	牧（まき）　徳達（のりみち）（愛知県）
学位の種類	博士（理学）
学位記番号	博甲第5617号
学位授与年月日	平成23年3月25日
学位授与の要件	学位規則第4条第1項該当
審査研究科	数理物質科学研究科
学位論文題目	**On applications of prehomogeneous vector spaces** （概均質ベクトル空間の応用について）

主査	筑波大学教授	理学博士	木村達雄
副査	筑波大学教授	理学博士	森田純
副査	筑波大学准教授	博士（数学）	増岡彰
副査	筑波大学准教授	理学博士	酒井克郎

論文の内容の要旨

牧　徳達氏は本論文に於いて、概均質ベクトル空間の理論の応用に関することを二つしているが、一つ目は大島利雄氏がある種の概均質ベクトル空間から超幾何関数が構成されることを示し、その空間の分類をしてほしいという要請に答えたもので、これは5名の共同の仕事であるが、牧　徳達氏は、あるタイプの有限軌道同値性を発見し、それが分類する上で大変役にたったので、貢献度は大きい。

もうひとつは、かつてドイツのポップ教授などが、概均質ベクトル空間の理論は暗号理論に使える筈だ、と筑波大学でのセミナーなどで話されていたことに刺激されて、牧　徳達氏が単独で色々考えて、暗号理論の中でも鍵共有のところでの応用の可能性を提唱したことである。

基本原理はある空間に群が作用しているとき、空間の基点を固定しておいて、群の元を与えれば、それを基点に作用させて空間の点がすぐに求まるが、空間の点を最初に与えて、基点からその点へ移す群の元を求めるのは難しいであろう、ということである。

その空間は何でも良いが実用上は線形代数が使えるのが望ましいので、ベクトル空間とするのが自然である。ただベクトル空間に線形代数群などが作用するという状況では、原点は動かないので、ベクトル空間自体が群の軌道になることはあり得ない。しかしながら、この問題の設定では基点と他の点は同じ群軌道に属すわけで、軌道が小さいと点の存在範囲がせばまってこの原理が活用出来なくなる。したがって我々が望むのは可能な限り大きな群軌道をもった状況であり、それは稠密な群軌道が存在することである。したがってここに自然に概均質ベクトル空間が現れる。

群の元が空間の点を与えたときに一意的に定まるためにはその概均質ベクトル空間の生成的等方部分群が単位群であることで、たとえば結合的代数の概均質ベクトル空間はそれをみたす。これは望ましい条件ではあるがかならずしも必要ではない。概均質ベクトル空間とその生成点が公開され、A、B、Cがそれぞれ群の元を秘密で持ち、それを与えられた生成点に作用させて得られる点を公開する。例えば群が可換ならば、AとBはそれぞれ相手の公開した元に自分の秘密の群の元を作用させれば、AとBは空間の元を共有し、それはCはわからない。このような概均質ベクトル空間の例としては可換フロベニウス代数の概均質ベク

トル空間がある。しかし可換でなくても交換子群の軌道を考えれば同じようなことが成り立つことも示した。

審 査 の 結 果 の 要 旨

いままで裏返し変換をはじめとして色々な概均質同値性は発見されていたが、有限軌道同値性はひとつも見つかっていなかった。超幾何関数への応用のある概均質ベクトル空間は有限軌道をもつ条件があるために今までの概均質同値条件を使うことは出来なかったが、牧　徳達氏は、ある種の有限軌道同値性を発見し、それが分類の完成に大いに役立ったことは評価できる。

また概均質ベクトル空間を暗号へ応用することを初めて具体的に提唱したことは、その道をきり開く可能性を示したことで大いに評価できる。以上により博士論文として充分な内容を持つものと評価出来る。

よって、著者は博士（理学）の学位を受けるに十分な資格を有するものと認める。